Cygna Auditor for SQL Server

User Guide

Cygna Auditing & Security Suite

For the latest information, visit online documentation at docs.cygnalabs.com

Published 1/11/2022

Version 5.9

Table of Contents

Introduction to Cygna Auditor for SQL Server

Note for BeyondTrust Customers

Cygna Labs assures BeyondTrust's Auditor Suite customers continuity with on going product development, maintenance and support. Please find the information below on respective name changes.

Former name	Current name
PowerBroker Auditor for Active Directory BeyondTrust Auditor for Active Directory	Cygna Auditor for Active Directory
PowerBroker Auditor for Exchange BeyondTrust Auditor for Exchange	Cygna Auditor for Exchange
PowerBroker Auditor for File System BeyondTrust Auditor for File System	Cygna Auditor for File System
BeyondTrust Event Vault for Windows	Cygna Event Vault for Windows
PowerBroker Auditor for SQL Server BeyondTrust Auditor for SQL Server	Cygna Auditor for SQL Server
Change Manager for Active Directory	Cygna Change Manager for Active Directory
Privilege Explorer for Active Directory	Cygna Privilege Explorer for Active Directory
Privilege Explorer for File System BeyondTrust Privilege Explorer for File System	Cygna Privilege Explorer for File System
Protector for Active Directory BeyondTrust Protector for Active Directory	Cygna Protector for Active Directory
Recovery for Active Directory	Cygna Recovery for Active Directory

Product Overview

A single change can put your critical applications and data at risk, affecting productivity, risking security breaches, and threatening non-compliance. Built-in SQL Server auditing capabilities are cumbersome, cryptic, and lack centralized auditing and reporting. Careful analysis of distributed logs requires enormous resources and still fails to paint the entire picture of SQL activity. Cygna Auditor for SQL Server brings a new level of centralized control and ease to SQL Server auditing and compliance. This powerful solution monitors all SQL Server activity in real time, tracking the who, what, where, and when information for every change.

Cygna Auditor for SQL Server Features

- Real-time monitoring of SQL Server environments, including changes to server configurations, security, databases, etc.
- A central audit database for reporting and alerting against all change activity
- An extensive library of security and compliance reports
- Intuitive wizards for custom views and reports
- Provides the originating IP address for each change
- Intelligent auditing that displays a single entry for every event
- Filtering, searching and reporting at the attribute level
- Audit event analytics for every object
- Single-click access to the change log of every SQL Server change event
- Does not require native event configuration or event logs
- Seamless integration with the full suite of Auditor products

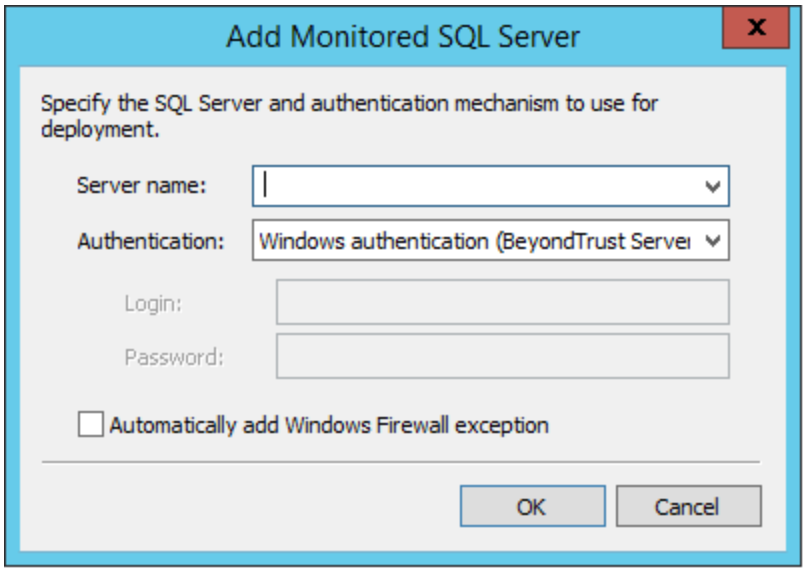
Configure SQL Server Monitoring

Requirements

- Cygna Auditor for SQL Server supports Microsoft SQL Server 2005-2017 environments.
- The Management server service account needs the sysadmin role on the SQL instance to be monitored and on the Auditor for SQL instance.
- The Microsoft SQL server process, on both the Auditor for SQL database server and the database server being monitored, must run as NT Authority\NetworkService or a domain user (preferred). The syntax is: domain\username or username@domain (.\username will not work). Running the service as LocalService is not supported because it presents anonymous credentials on the network.

Add a SQL Server for Monitoring

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Expand the **Auditor for SQL Server** node.
4. Click the Servers node.
5. Right-click in the working area and select Add Monitored SQL Server. Alternatively, right-click the Servers node and select Add Monitored SQL Server.
6. To add a server, click Add.

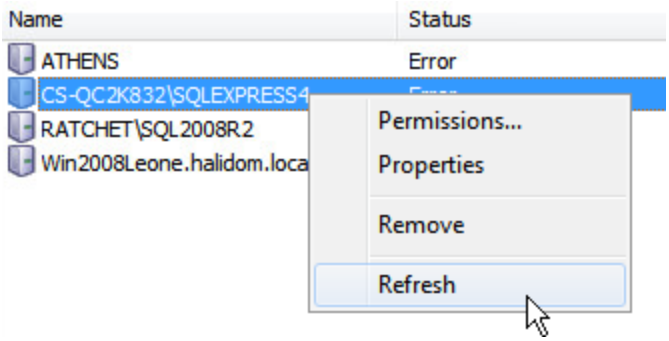


7. In the Add Monitored SQL Server dialog box, complete the fields as follows:
    - Server name: The name of the SQL Server instance. SQL servers on the network are available in the list.
    - Authentication: Select an authentication type for the installation of the monitor. The selected account must be a member of the SQL Server sysadmin role. There are three options.
        - Windows authentication service credentials.
        - Windows authentication (specified): Enter the login and password. If the Management Server is running as Local System, using this option will not work. You must enter credentials.
        - SQL Server Authentication: Enter the login and password. Note that if this option is used, the Management Server service account is used to access the file system of the remote SQL Server. This account must have administrative privileges for the remote SQL server.
    - **Automatically add Windows Firewall exception**: Select the check box to allow communication to and from the SQL Server.
8. Click OK to add the server to the monitoring list.
9. Click **Add** to add another server to the monitoring list.
10. Click **OK** to start monitoring the SQL servers. The server status is displayed in the working area.

View SQL Server Status

To view the status of monitored SQL Servers:

1. Expand the **Auditor for SQL Server** node.
2. Select the Servers node.
3. There are three status states:
    - Deploying when monitoring is being set up.
    - Active when setup is complete and monitoring is taking place.
    - Error if an error occurs during setup.

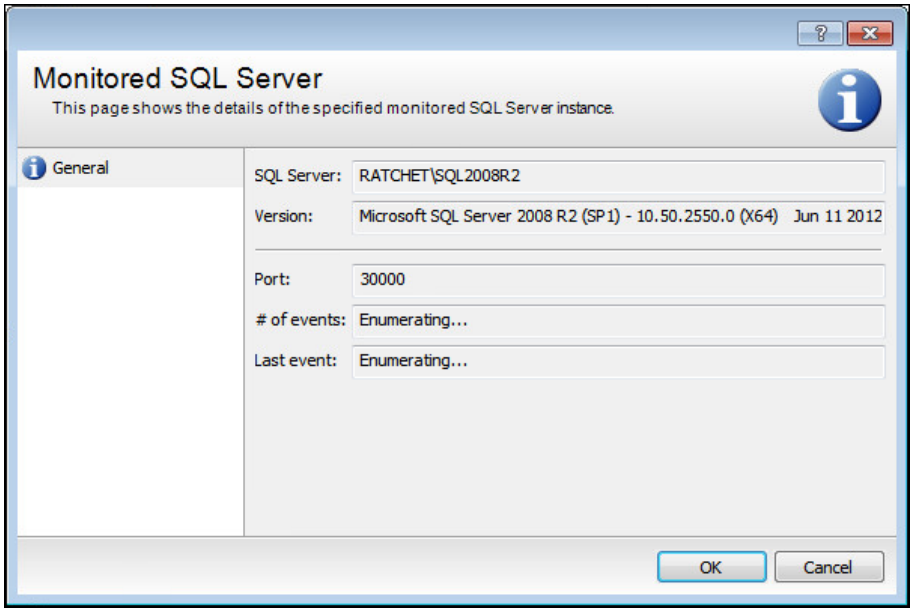


4. To refresh a server's status, right-click the server, and then select Refresh.

View Properties of Monitored SQL Servers

To view a server's properties:

1. Expand the **Auditor for SQL Server** node.
2. Select the Servers node.
3. Right-click the server in the working area and select Properties.



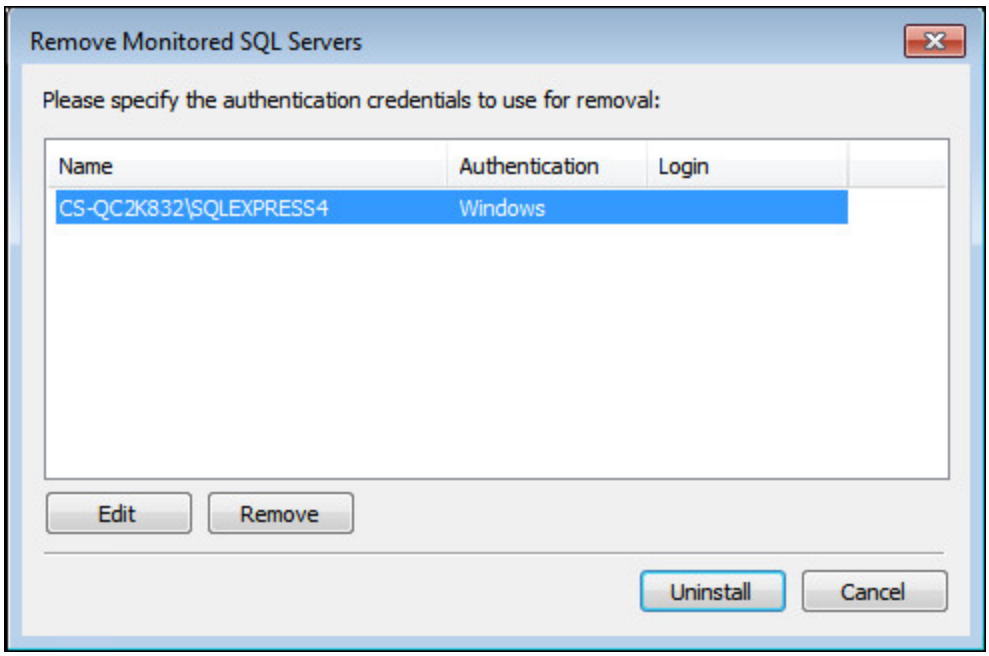
4. The details in this dialog box include:
   - SQL Server: The name of the SQL server being monitored.
   - Version: The version of the SQL server being monitored.
   - Port: The port that the monitored SQL server is using to communicate with the Auditor for SQL database.

- # of events: The number of monitored events from this SQL server.
- Last event: The time of the last monitored event.

Remove a SQL Server from the Monitoring List

To stop monitoring a SQL Server:

1. Expand the **Auditor for SQL Server** node.
2. Select the Servers node.
3. Right-click the server, and then select Remove.
4. Click Yes.



5. Confirm the servers to remove and the credentials used.
   - Edit opens the Authentication dialog box and allows you to change the credentials. By default, Auditor for SQL uses Windows Authentication using the Auditor for SQL service credentials.
   - Remove removes the server from the list to be uninstalled.
6. Click Uninstall to remove the selected servers from the monitoring list.

Work with Alerts

Cygna Auditor for SQL Server can alert users via email when certain events are logged. The event details are then sent via email to the specified accounts in HTML format. Note that Auditor for SQL Server uses the global email settings for sending email alerts.

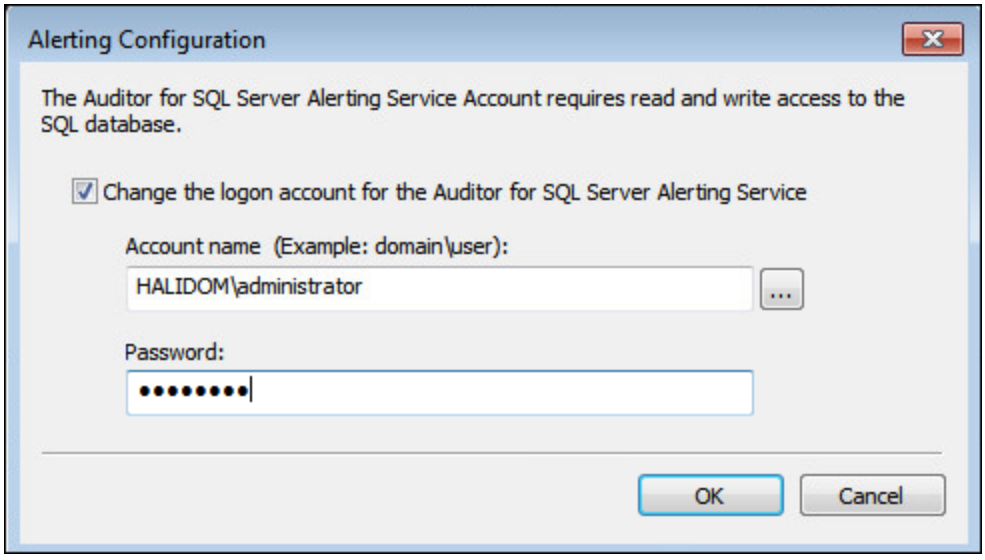
For more information, please see Configure Email Notification.

Configure the Alerting Service

By default, there is no logon account configured for the Auditor for SQL alerting service.

To configure the account:

1. Select the Auditor for SQL Server node.
2. If alerting is not configured, a message displays.

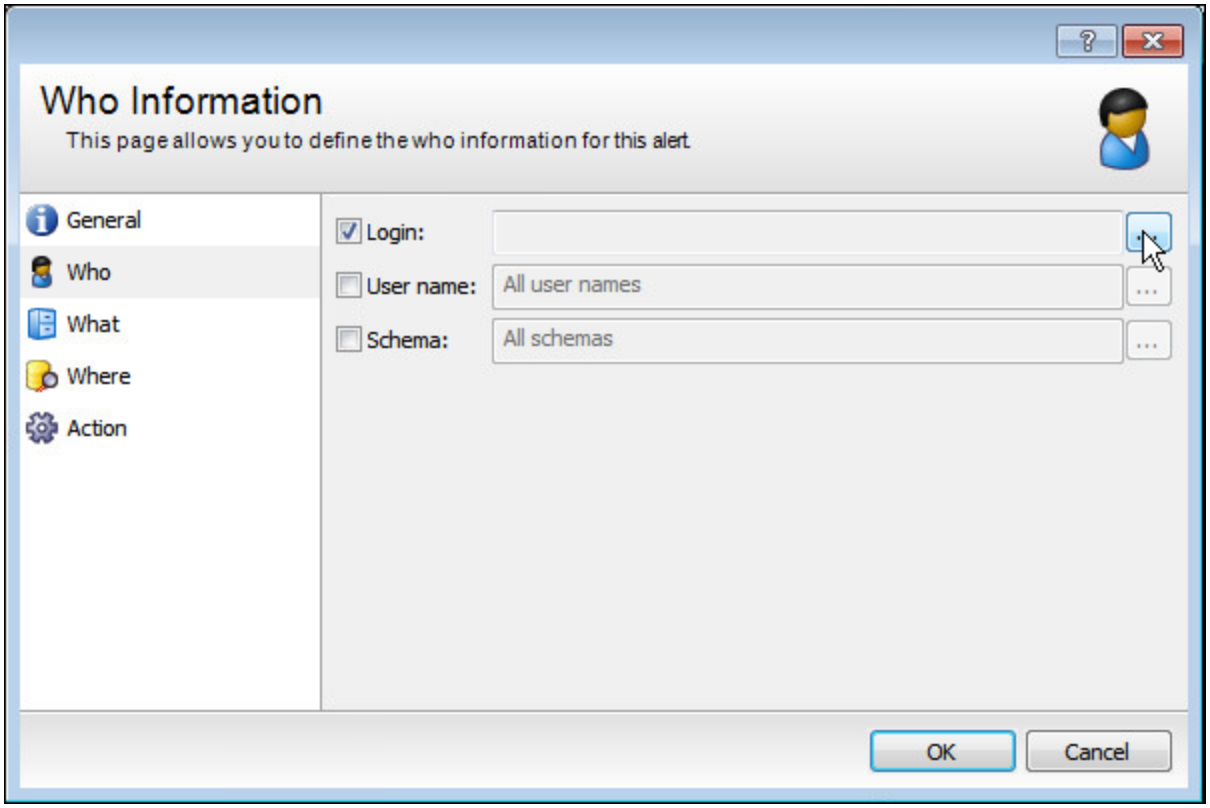


3. Click the hyperlink to display the Alerting Configuration dialog box. You can enter or change the logon credentials for the alerting service.
4. Click OK.

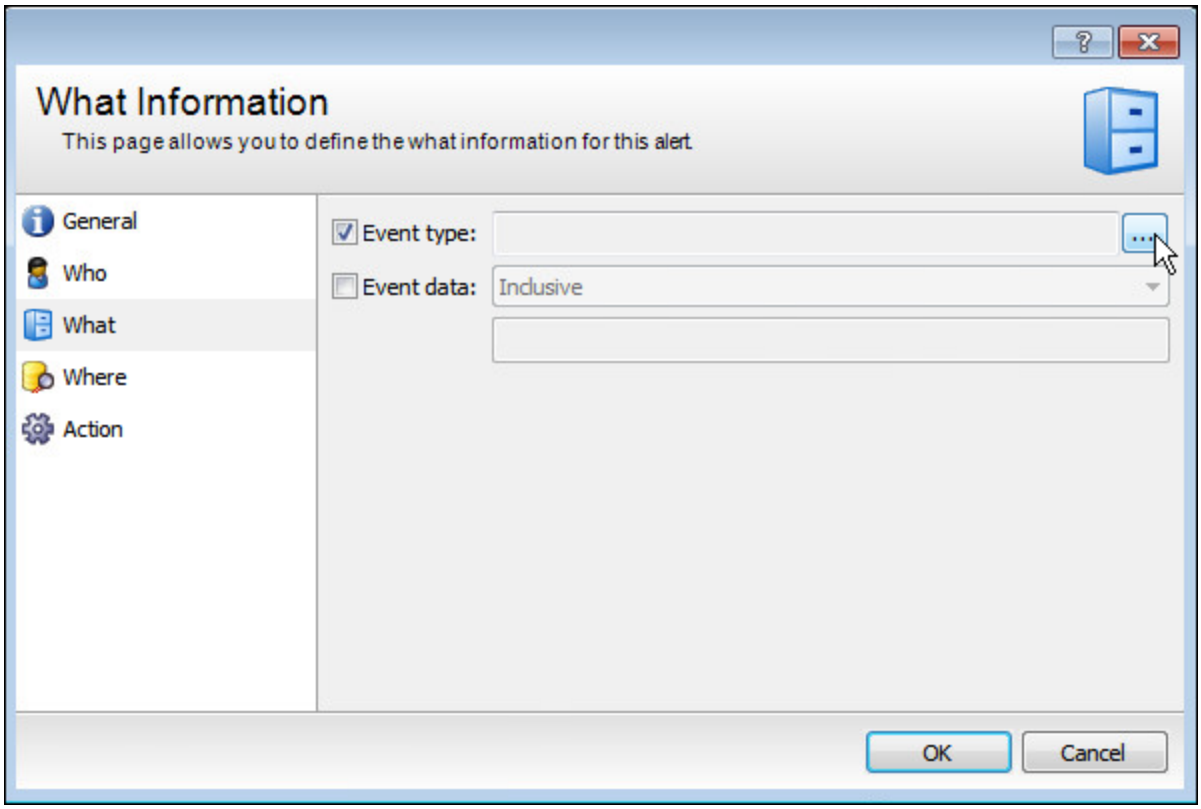
Create Alerts

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Expand the **Cygna Auditor for SQL Server** node.
4. Right-click Alerts, and then select New > Alert.

5. On the General page, provide a name and description for the alert.
6. Select the The alert is enabled check box to turn the alert on or off.
7. On the Who page, select logins, user names, and schemas to alert on. By default, all items are included.

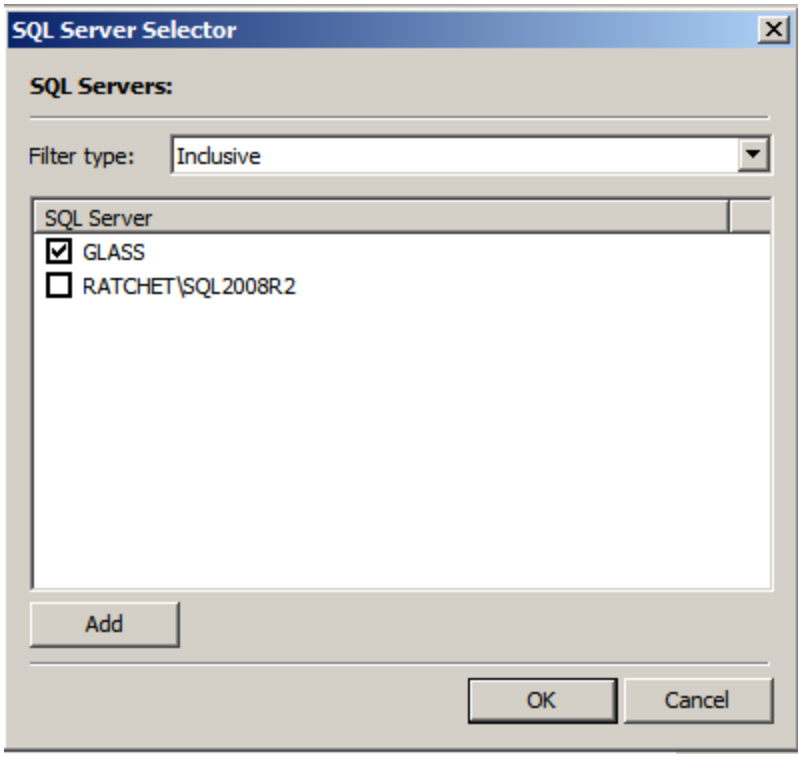


8. To choose an item, select the item and click the Browse button.
9. On the selector dialog box, select a filter and select items to include or exclude. Items with audit data are in the list.
10. To add items, click Add, type the new item name and press Enter.



11. On the What page, select event types to alert on. By default, all items are included. Select the Event type box and click browse.
12. Select a filter type and select the events to include or exclude. Items with audit data are in the list.
13. To add items, click Add, type the new item name and press Enter.
14. You can also filter on advanced event information such as custom data for a specific event that is not available in the other page. Select Event data and select the filter type: Inclusive or Exclusive.
15. Enter the criteria to include or exclude in the field below the Event data menu.
16. On the Where page, select the server, database, or objects to alert on. By default, all items are included.

17. To select items, check the item and click Browse.

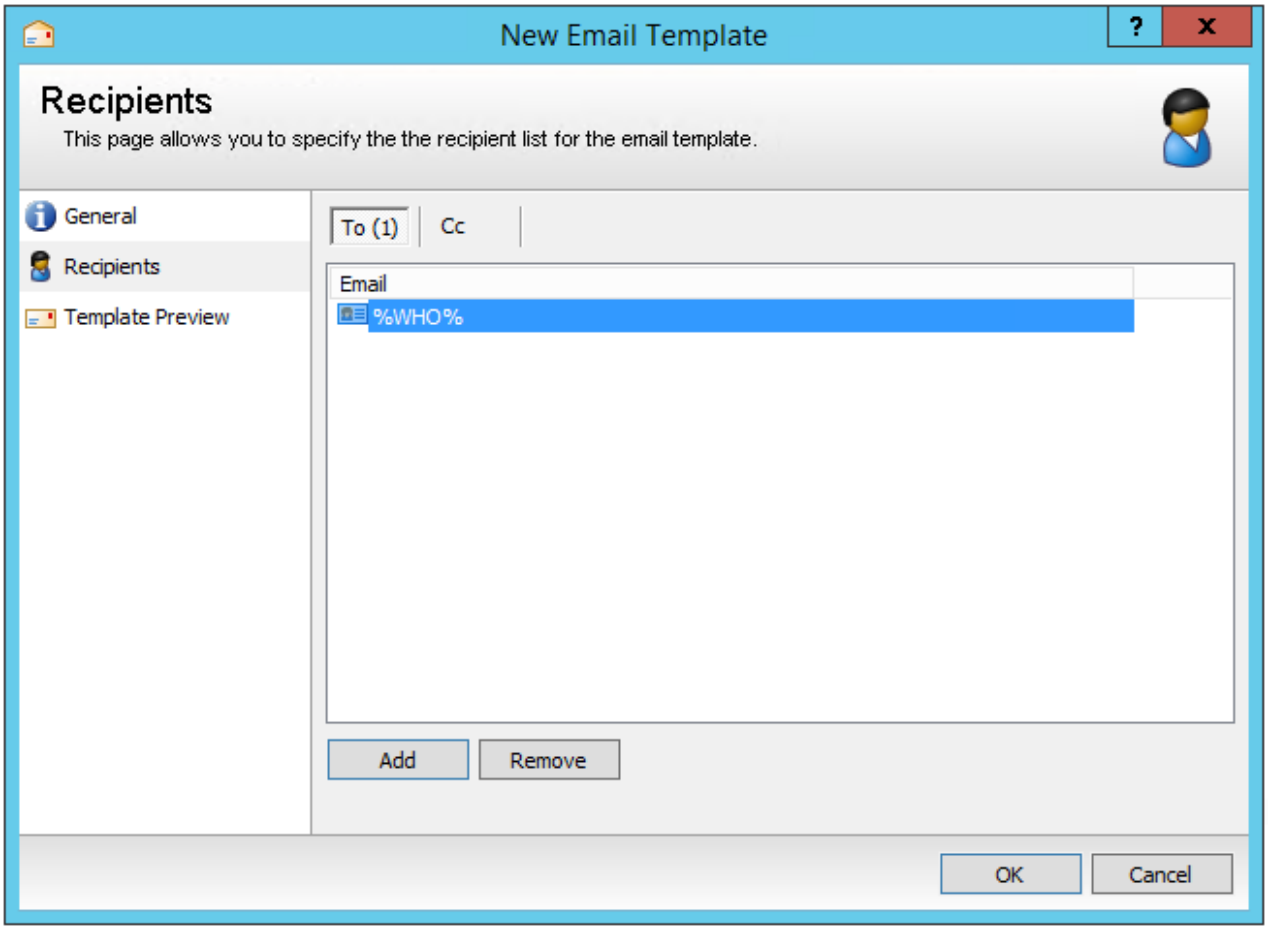


18. Select the filter type: Inclusive or Exclusive. Servers that have been audited are in the list. Select items to include in the view, and then click Add.
19. Type the new item, and press Enter.
20. On the Action page, click Add to enter email addresses to send the alerts.
21. Select from the following alert types. You can select more than one alert type.
    - Write to event log: Writes an event to the event log on the Management Server.
    - Send an alert to: Email addresses that receive the alert. Enter more than one email by separating the addresses with a semicolon. For more information, please see Email Templates.
    - Send SNMP message: Sends a network message with the alert details. Any SNMP monitoring application can receive it.
22. After you finish setting alert options, click OK.

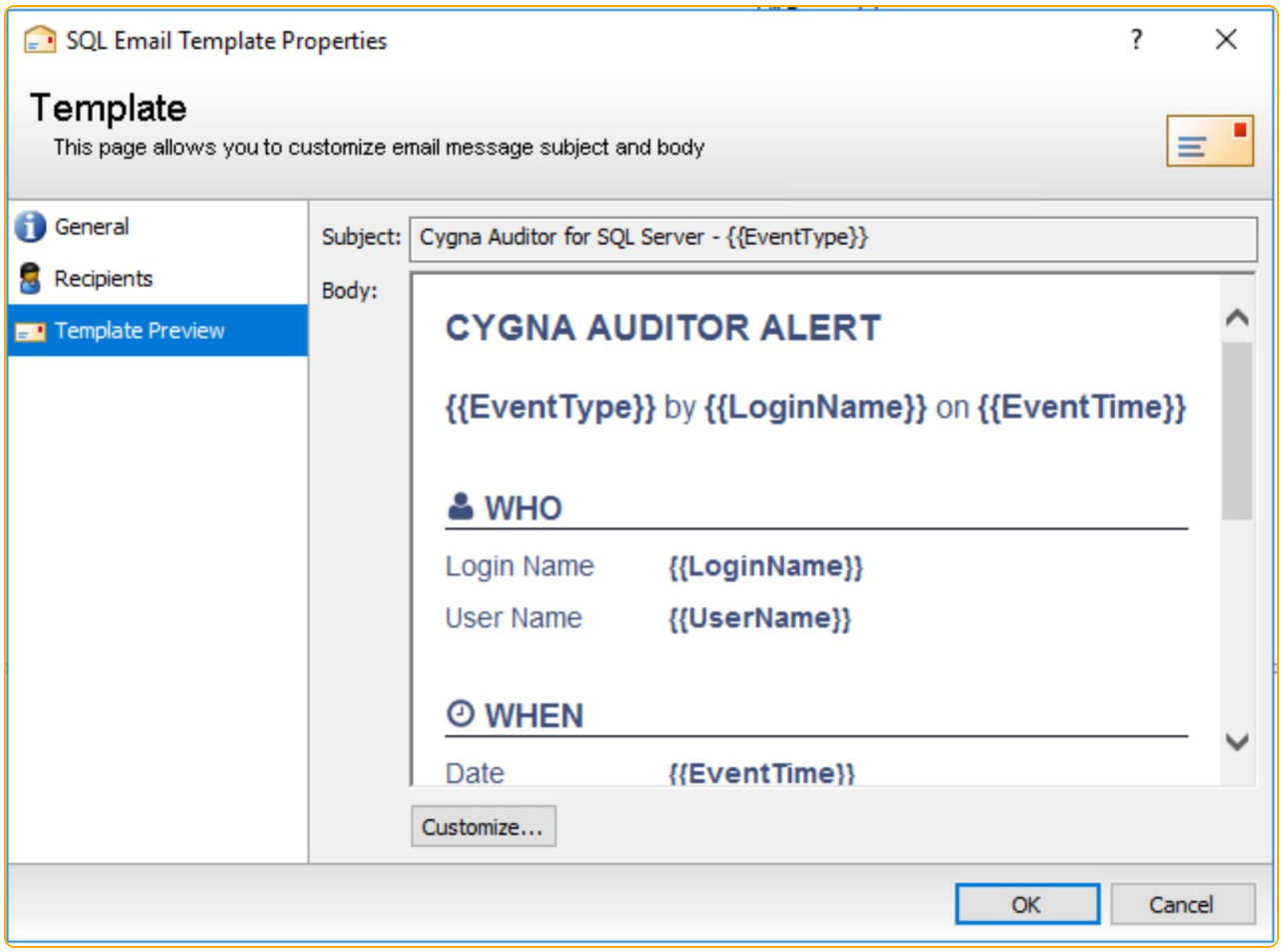
Email Templates

When you set up alerts, you can choose to email a recipient with the alert details or create an email template.

1. In the console, expand Configuration > Email Templates.
2. Right-click the node for the module you want to create the template for. For example, SQL Server Alerts.
3. Provide a name and description for the template.
4. Select the Recipients tab, and then click Add to enter recipients.



Administrators can enter the %WHO% wildcard to send an email to a user that exists in Active Directory. This email notifies the user of the changes they made.



5. Select Template Preview.
6. Click Customize to change the template.
7. On the HTML tab, you can modify the text in the window or you can click Source to modify the HTML code. You can also import and export .html files. The Import and Export buttons are enabled when you click Source.
8. Click OK.
9. After you finish configuring the template, click OK.

Modify and Delete Alerts

Modify Alerts

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Expand the **Auditor for SQL Server** node.

4. Click the Alerts node.
5. Right-click the alert and select Properties.
6. Change the settings and click OK.

Delete Alerts

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Expand the **Auditor for SQL Server** node.
4. Select the Alerts node.
5. Right-click the alert and select Delete.
6. Click Yes to confirm your action.

Configure Email Notification

To send email alerts, you must configure the SMTP settings for Auditor.

1. Start the console.
2. Expand Cygna Auditing & Security Suite.
3. Expand Configuration.
4. Select the General Settings node.
5. The Email Settings are blank until they are configured. Click Edit to configure each section.
6. When the Email Settings dialog box opens, enter a name in the Display Name box.
7. Type an email address in the Email Address box.
8. Type the name or the IP address of the SMTP server. If necessary, select the Use logon information box and enter credentials for the SMTP server. Security Protocol:
   - None: Creates an unencrypted connection on the specified port (default 25).
   - SSL: Creates a secure connection using SSL (Secure Sockets Layer) encryption on the specified port (default 465). Requires SSL, otherwise the connection fails. SSL and TLS connections require credentials.
   - TLS: Creates a secure connection using TLS (Transport Layer Security) encryption on the specified port (default 587). Requires TLS, otherwise the connection fails.
   - Check for server certificate revocation: If selected, enforces a server certificate revocation check before sending email alerts. This requires internet access for the

machines where AS Server, MMC, and agents are deployed; otherwise checks fail and no email alerts are sent.

9. After you enter this information, click Test to ensure the settings are working correctly. A test message is sent to the email address provided.
10. Click Save.
11. After you save your configuration, the information appears when you select the General Settings node.

To turn off email notifications, un-check Enable email settings and click Save.

Troubleshoot Email Notifications

If you have trouble receiving your email notifications, please note the following:

- Both DCs and the Management Server need permission to send.
- DCs must be on the allowed list for the SMTP server to accept an email from them.
- The DC must be able to communicate with the SQL Server to pick up SMTP settings.
- The DC must be able to communicate with the SMTP server to send the notification.
- On the Email Configuration page, ensure you test the settings.

About Audit Views

An audit view is a collection of SQL Server audit events you want to view. You can open the Audit Viewer window to review and analyze the results.

Packages I Need to Use This Feature

Module	Description	License Required?
Server/Console	The Server/Console module provides fundamental setup features such as deploying agents; configuring email accounts; and creating schedules to associate with collectors, policies, and auditing.	✓
Auditor for SQL Server	The Auditor for SQL Server tracks changes to SQL objects. Each audit event includes the who, what, where, and when information for all changes. It also includes before and after values for all attributes. The Audit Viewer, built-in audits, and creating collector policies are key features provided by the auditor module	✓

Audit View Search Filter

Search the Audit View list using the search filter provided at the top of the window. Audit Views can be searched by name using keywords.

Built-in Audit Views

Under the Audit Views node, you will see two folders: Built-in and My Audit Views. Auditor for SQL ships with a complete set of pre-built audit views for you to use.

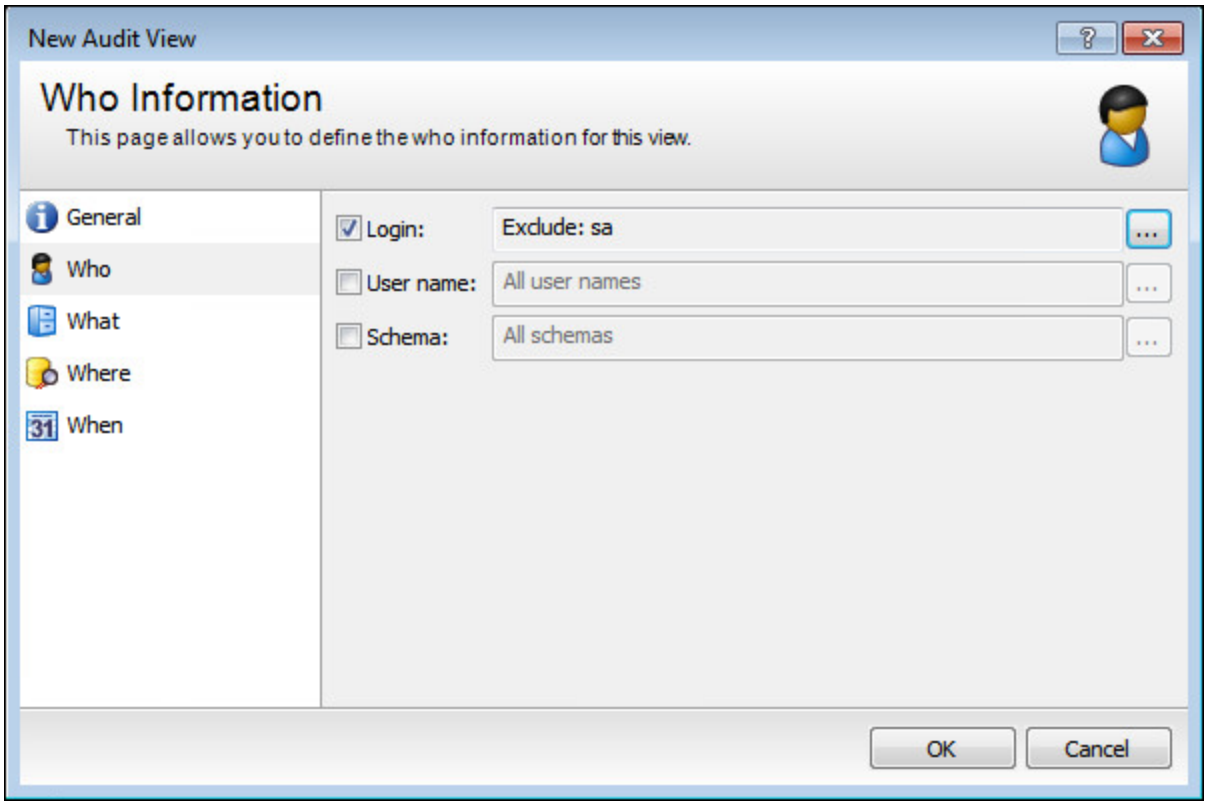
The folder labeled My Audit Views is a private user account folder. Any views or subfolders created under this folder are only accessible by the user who created them.

Name	Description
All Changes in Last 24 Hours	View all SQL server audit activity from the past 24 hours.
Deleted SQL Server Objects	View deleted objects, such as tables, indexes, and procedures.
Failed Login Attempts	View failed login attempts. Useful for identifying possible security breach attempts and troubleshooting login failures.
Function Changes	View all creations, deletions, and modifications performed on functions.
Index Changes	View all creations, deletions, and modifications performed on indexes.
Modified SQL Server Objects	View modified objects, such as tables, indexes, and procedures.
Newly Created SQL Server Objects	View objects, such as tables, indexes, and procedures created in the past seven days.
Procedure Changes	View all creations, deletions, and modifications performed on functions.
Server Instance Changes	View changes to the SQL Server global configuration settings. Not available for SQL Server 2005.
Server Role Changes	View when members have been added to or removed from a SQL server role.
User Changes	View all creations, deletions, and modifications performed on users.
View Changes	View all creations, deletions, and modifications performed on views.

Create an Audit View

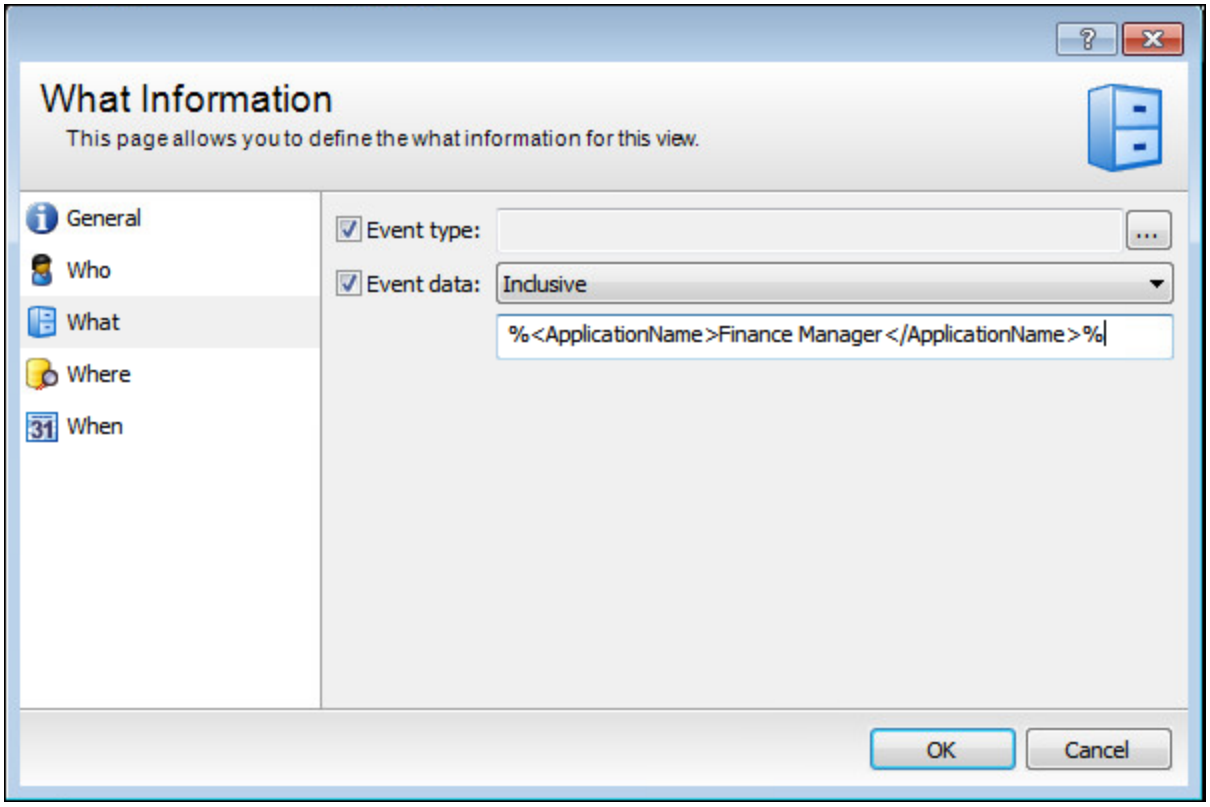
If any of the available templates do not suit your requirements, you can customize audit views to meet your specific needs.

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Expand the **Auditor for SQL Server** node.
4. Select the Audit Views node.
5. Right-click in the working area and click New > Audit View.
6. After you enter your settings, click OK.
7. On the General page, provide a name and description for the view.

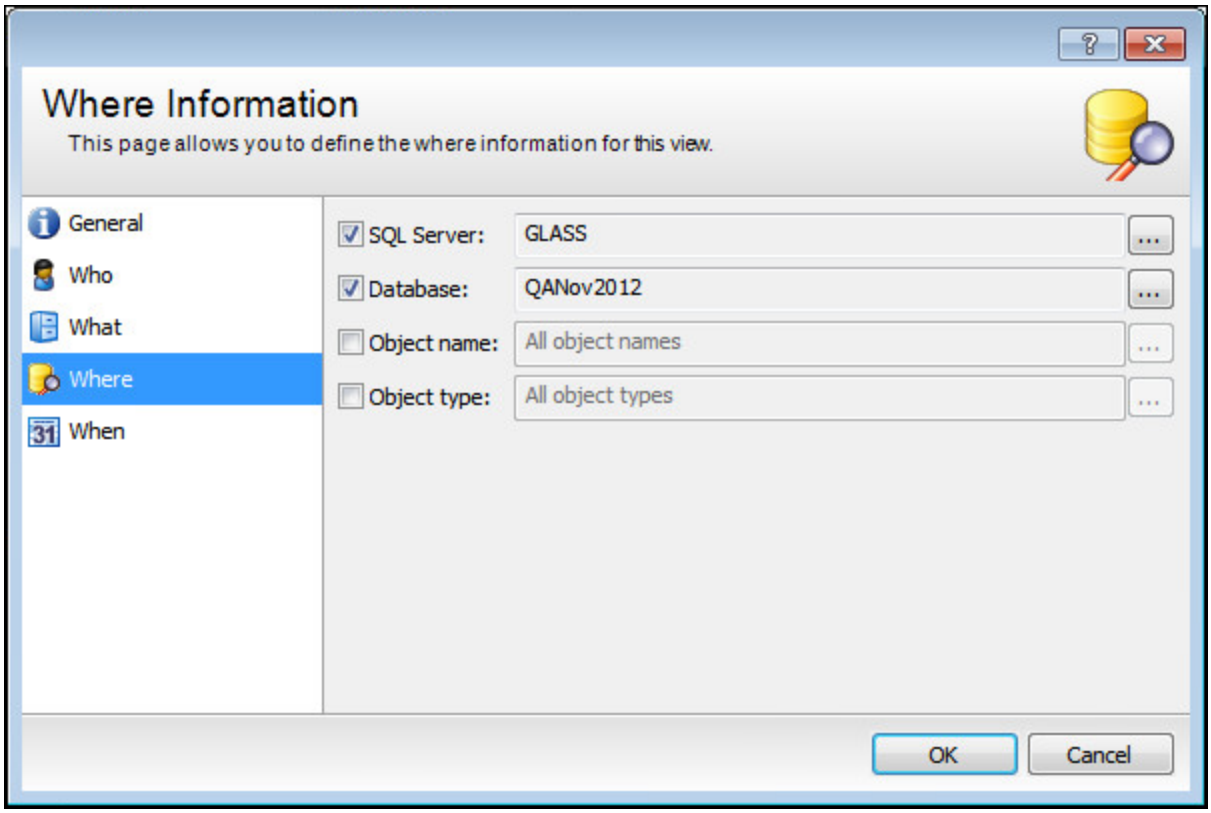


8. On the Who page, select logins, user names, and schemas you want to view audit data for. By default, all items are included.
9. On the selector dialog box for the object type, select a filter type and select the items to include or exclude. Items with audit data are in the list.
10. To add new items, click Add, type the new item and press Enter.

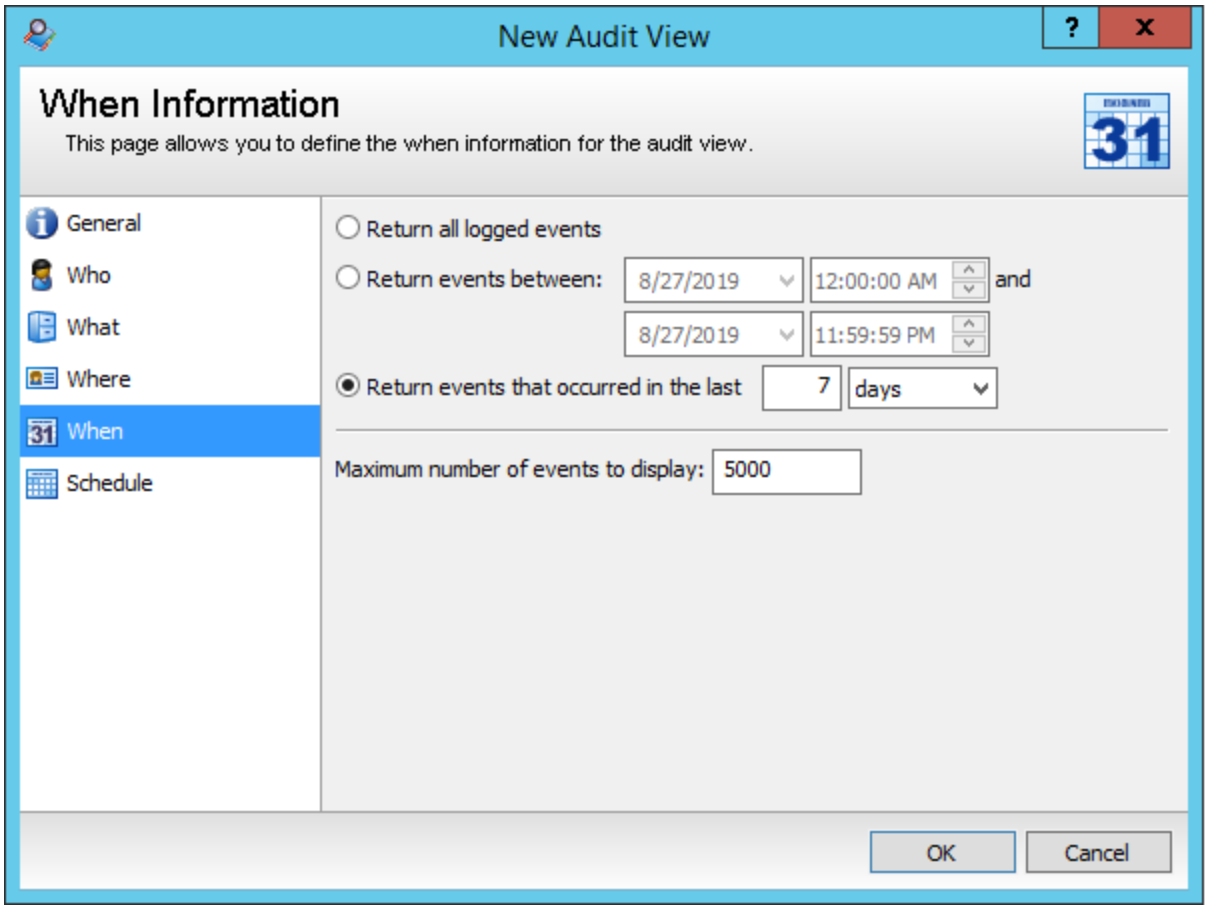
11. On the What page, select the Event type box to add event types to view audit data for. By default, all items are included.
12. Select a filter type and select the events to include in or exclude. Items with audit data are in the list.
13. To add items, click Add, type the new item and press Enter.
14. You can also filter on advanced event information such as custom data for a specific event that is not available in the other pages. Select a filter type: Inclusive or Exclusive.



15. Enter the criteria to include or exclude in the field below the Event data menu.



16. On the Where page, select server, database, or objects to view audit data for. By default, all items are included. To select specific items, check the item and click browse.
17. On the selector dialog box, select a filter type and select the items to include or exclude. Items with audit data are in the list.
18. To add items, click Add, type an item and press Enter.
19. Click OK.



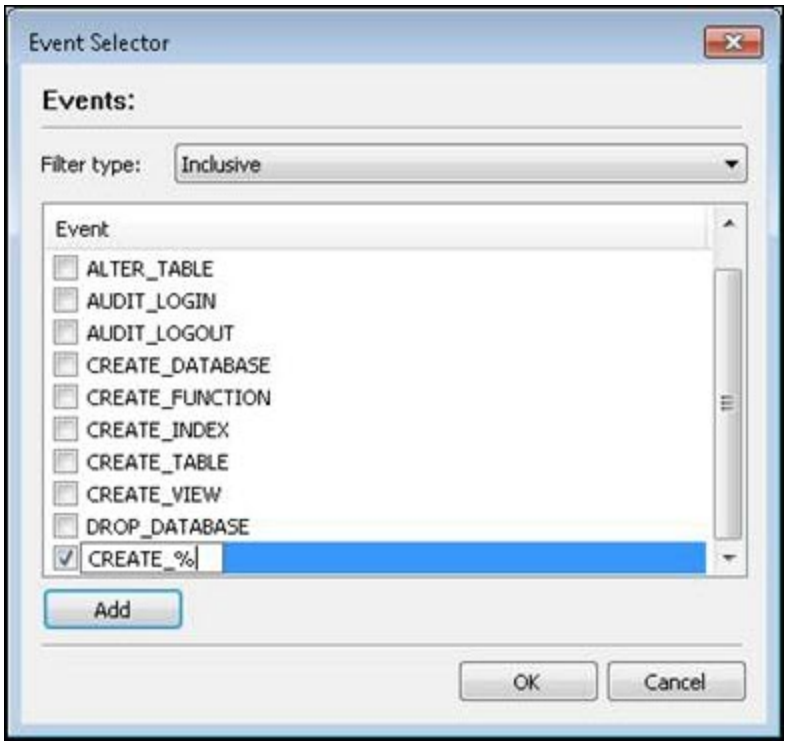
20. On the When page, select a date range from the following options:
    - Return all logged events: Select this option to display all logged events in the Audit Viewer window.
    - Return events between: Select this option, and then select date ranges from the date lists. This filters the list of logged events in the Audit Viewer window by date.
    - Return events that occurred in the last x <*time frame*>: Select this option, and then enter a value in the box. This filters the logged events that occurred in that number of days, minutes, hours, weeks, or months.

Using Wildcards

The Who, What, and Where pages support SQL wildcards (%).

- String%: returns values that begin with *String*
- %String: returns values that end with *String*
- %String%: returns values that contain *String*

For example, this entry in the Login Selector dialog box, from the Who page, includes all audit activity from logins in the BB2K8 domain.



This entry in the Event Selector dialog box, from the What page, includes all create activities.

Work with the Audit Viewer

Configure Access to the Viewer

Accounts must be added in the management console to see collected data in the Viewer. By default, no accounts are given audit permission. When you try to open an audit view before adding an account, an error message states you do not have access to view collected data.

Note: A user must be a member of a group or explicitly defined in the Auditor Accounts section, or they cannot run the Audit Viewer, even if appropriate permissions are in place for the view.

To add accounts:

1. Start the console.
2. Expand Cygna Auditing & Security Suite node.
3. Select the **Auditor for SQL Server** node.
4. On the dashboard, click the link to manage the list for viewing collected audit data.
5. Click Add.
6. Select the accounts to add, and then click OK.
7. Click OK.

Open Audit Views

1. Start the console.
2. Expand the Cygna Auditing & Security Suite node.
3. Expand the **Auditor for SQL Server** node.
4. Select the Audit Views node.
5. To open a default or user-created audit view, right-click the audit view and then select Open.
6. To open an audit view in a folder (such as a built-in audit view), double-click the folders in the main console window, or navigate through the tree on the left. Right-click the view, and then select Open.
7. When you open a view, you will see the Audit Viewer window.

Audit Viewer Window

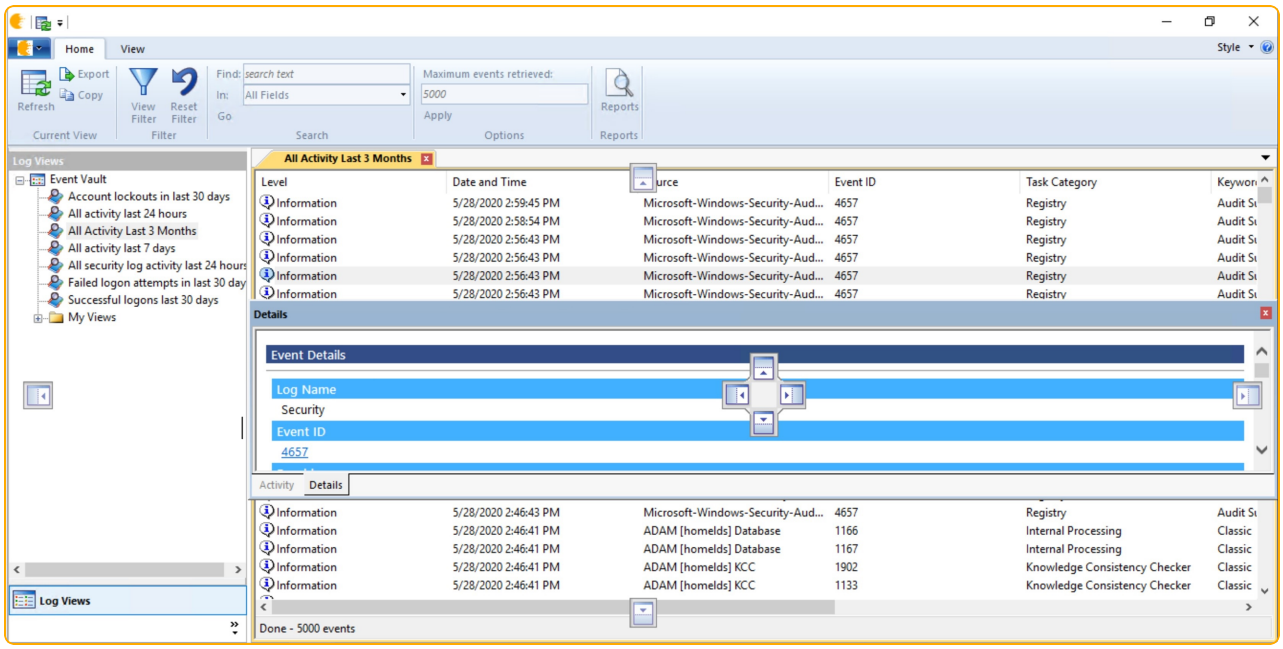
The Audit Viewer window displays the following details:

- A list of available views.
- The data retrieved based on the specifications of the audit view you created.
- The Who, What, Where, and Action filter information.

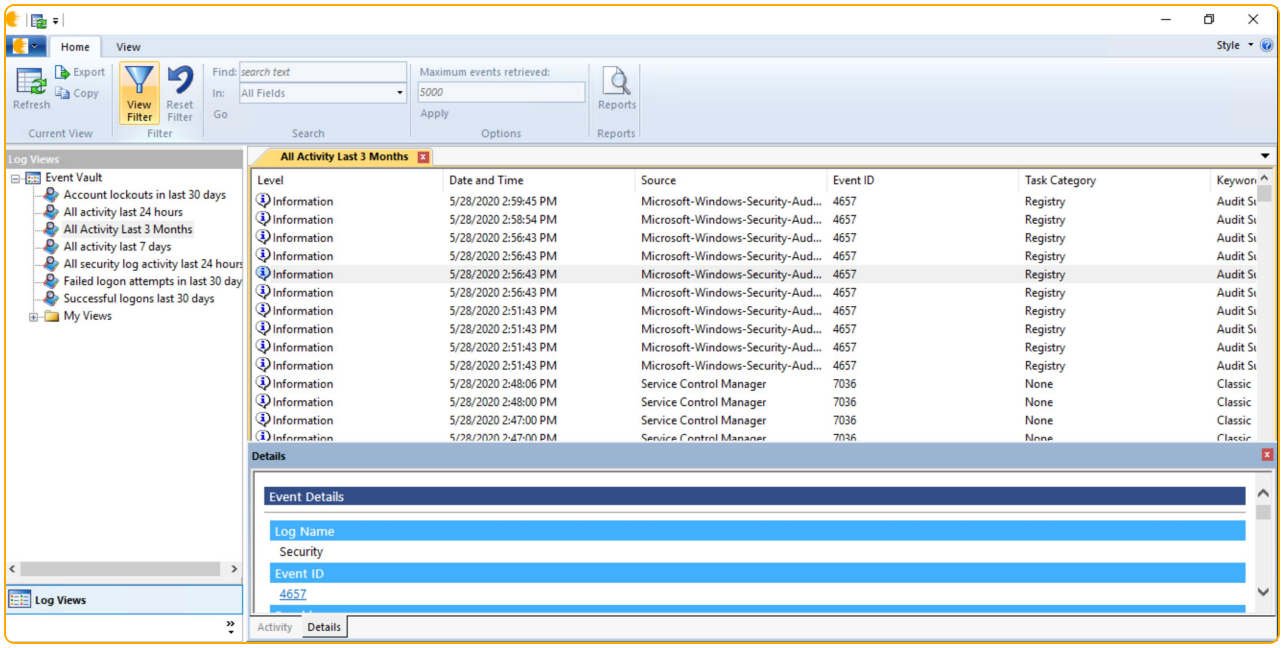
Here is an overview of the window.

- Open Audit Views: Displays the associated audit events based on the view and any applied filter settings. If multiple audit views are open, they are tabbed.
- Details: Shows information for the selected audit event.
- Activity Summary: Shows high level statistics about audit events in the environment. Use the tabs to view data on SQL server activity, account activity, event activity, or database activity for the currently selected view.

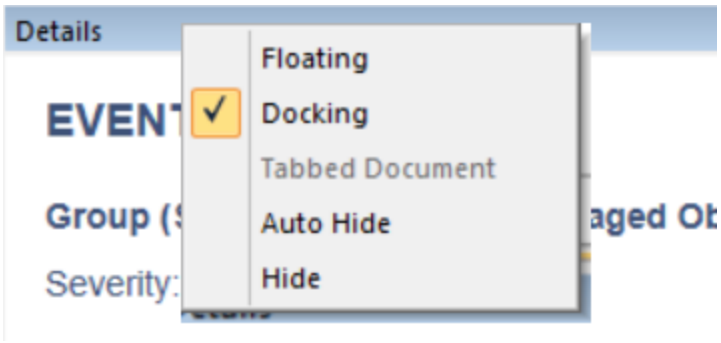
Customize the Audit Viewer Window



Drag and dock the title bars to customize the view. The panes can be resized to the desired width and height.



In the example, the Details pane is at the bottom of the window.



Right-click on the title bar to choose from Floating, Docking, or Hide options.

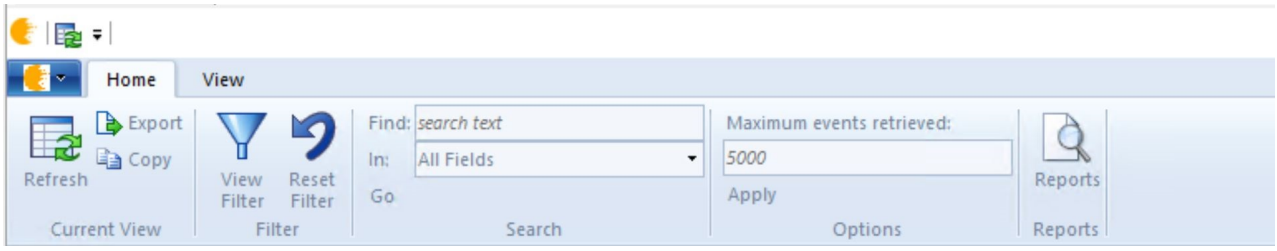
Use the Auditor Interface

The ribbon area below the title bar provides the following functionality.

Auditor Menu

- Export the current data.
- Close the current view.
- Exit the Viewer.

Home Tab



Current View

- **Refresh:** Updates the objects in the open view window.
- **Export:** Export object permission data to an XML or PDF file.
- **Copy:** Copy the contents of the selected objects for pasting into a document or email.
- Group Explorer: Provides controls to select a user/group, and a snapshot date from the available snapshots in the database.

Filter

- **View Filter:** Provides a way to refine the returned events to create a subset based on the categories of information that make up a view.

Search

- Find: Provides a way to search using keywords.
- **Reset Filter:** Undo any filter modifications to the original properties of the opened view.

Options

- **Maximum Objects Retrieved:** Enter the maximum number of objects to return.

Data Source

- Select Data Source: Select archived or current data.

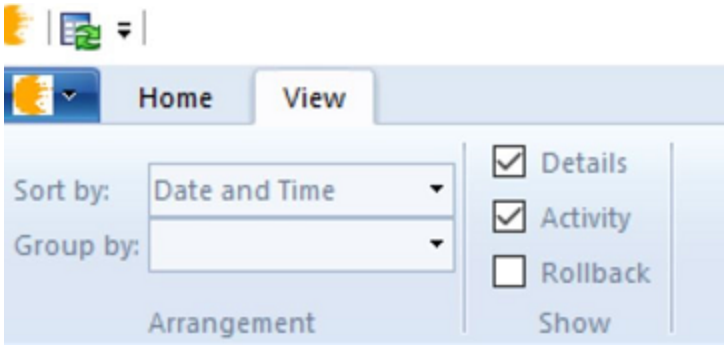
Reports

- Open Reports: Allows you to view the audit data in a published report, if reporting is configured with Microsoft SQL Server Reporting Services (SSRS).
- Publish: Allows you to generate a report for your audit data and publish to SSRS. Once published, it is then available to view in SSRS.
- Themes Layouts: Allows you to customize your report themes and layouts. For example, change report logo, report colors, and select columns.

Rollback

- Add to Queue: Add multiple events to the rollback queue and roll back all events at once.
- Rollback Now: Roll back the changes related to a single event.
- Show Queue: Display the events that are currently in the rollback queue, pending rollback.

View Tab



Arrangement

- Sort by: Select the column the events are sorted by.
- Group by: Select the column to group the events.

Show

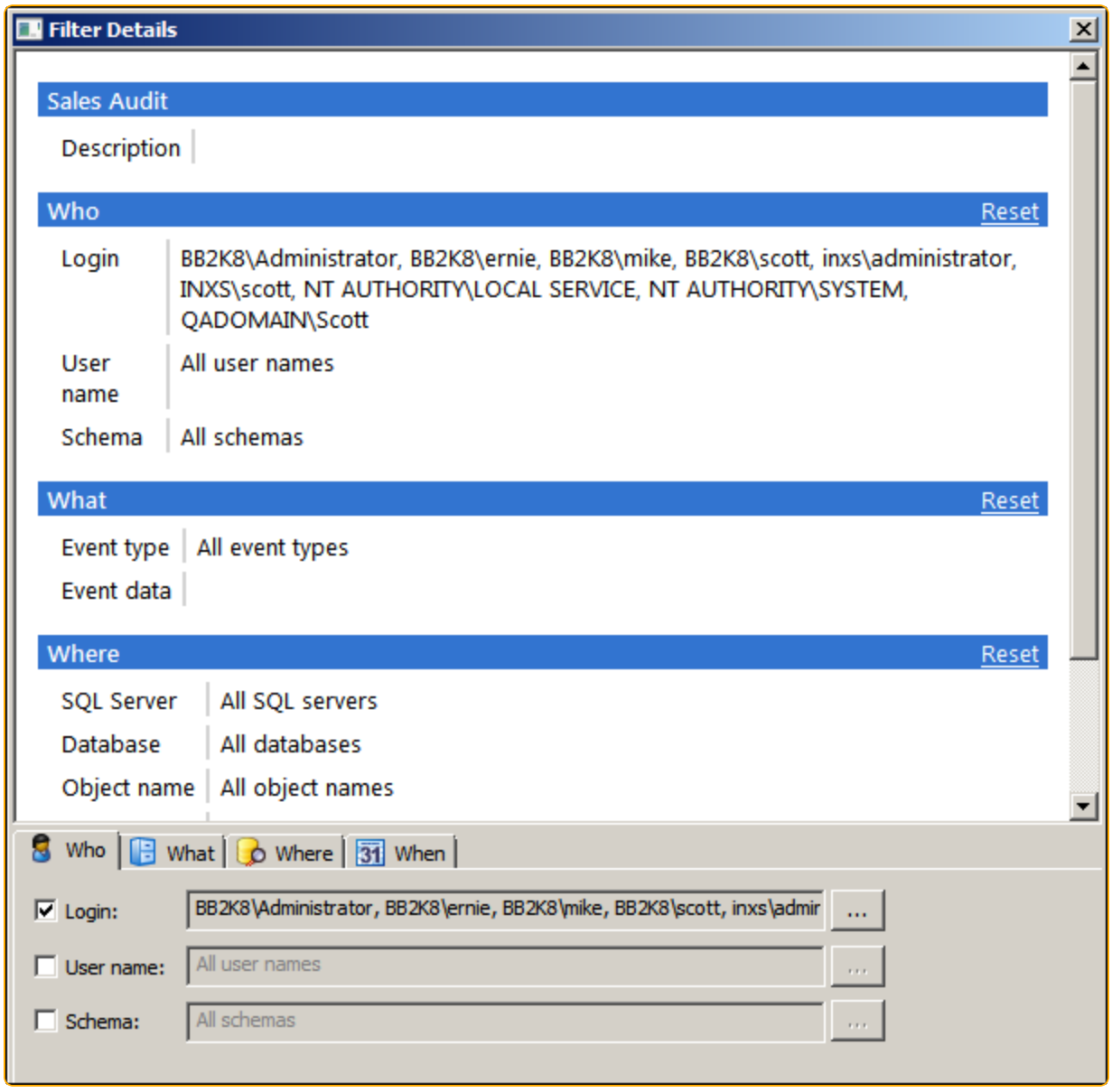
- Details: Check to display the Details window in the viewer.
- Activity: Check to display the Activity window in the viewer.
- Rollback: Check to display the Rollback Queue in the viewer.
- Style: You can change the look of the Audit Viewer window using the Style menu on the right side.

Change the Properties for an Audit View

You can temporarily change the properties for an audit view you created. When you change the properties on the Audit Viewer window, you can refresh the search results to display the values that meet the newly selected criteria. The changes are not permanently saved to the audit view.

Plan your auditing activities. To view relevant data, it is important to know the object types you want to monitor and the attributes for the objects.

1. Open the audit viewer in one of the following ways:
   - In the console, right-click an audit view you created earlier, and then select Open.
   - Select Start > Audit Viewer. Double-click a view in the Audit Views pane.
   - Run the viewer executable located in: \Program Files\BlackBird\Console\SQLAuditorViewer.exe.

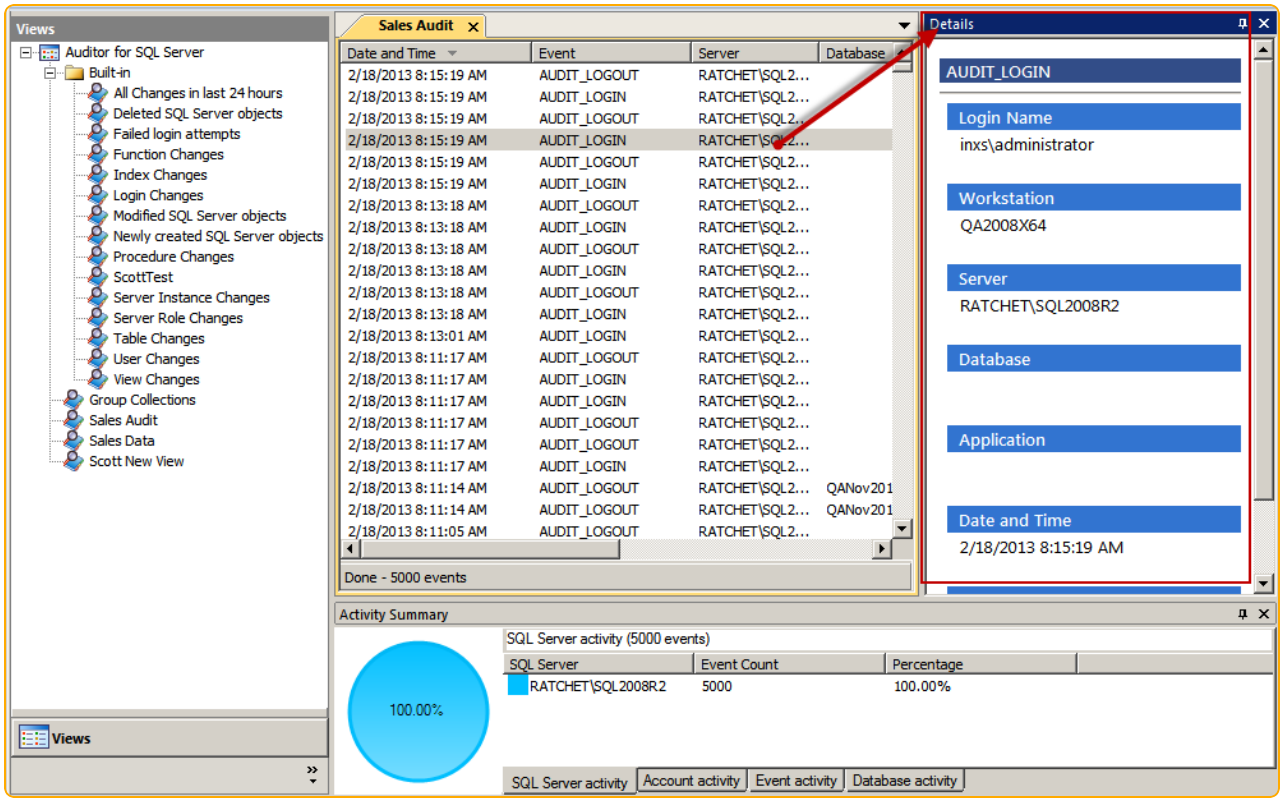


2. Click View Filter to open the Filter Details window. The current settings for the audit view are displayed.
3. Change the properties on the Who, What, Where, and When tabs.

For more information, please see the appropriate page in Create an Audit View.

4. Click Reset to change the settings to the previous values when you opened the Filter Details dialog box.
5. After you enter your settings, click OK. Resize the dialog box if you cannot see OK and Cancel.
6. The results are displayed in the Audit Viewer window.

Review Results



Select an audit entry from an open audit view to review more detailed information about the event. The information is displayed in the Details pane.

When reviewing audit information, you can:

- Click the columns to sort the information by that column.
- Group items by right-clicking in the workspace window, clicking Group by, and choose a criterion.

Use the Activity Timeline

To turn the Activity Timeline on or off, select an event and click Timeline on the Home tab.

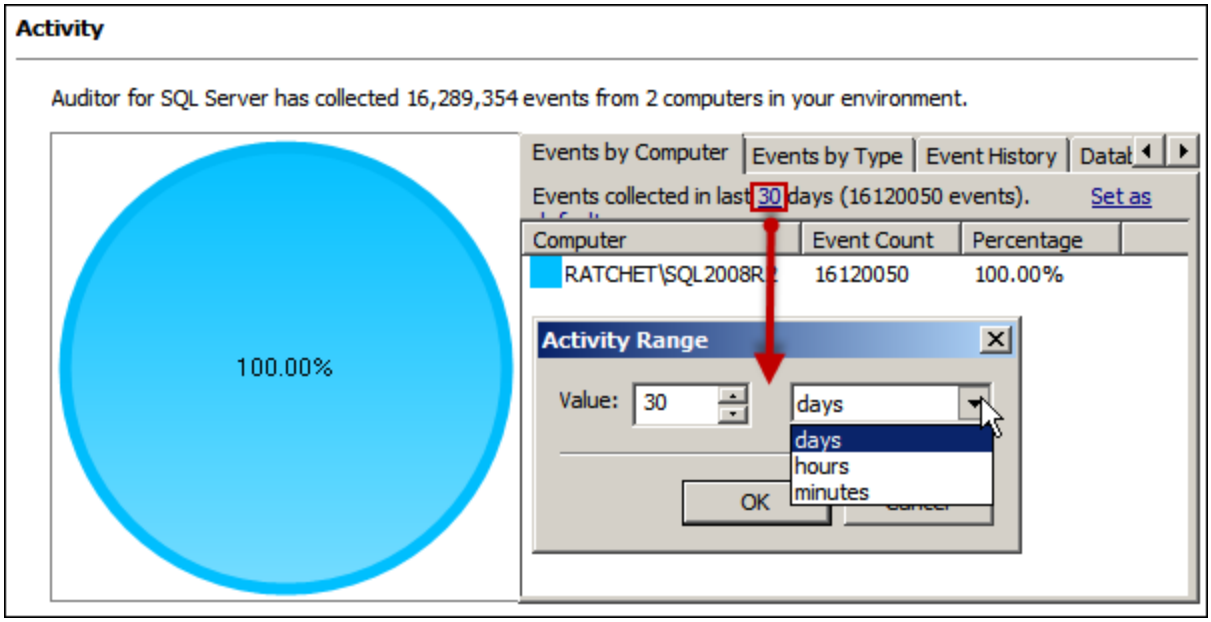
You will see all activity for that particular SQL Server session, from log on to log off and all events in between. Events outside the filter scope will be included.

Details view, grouping, sorting, and searching are available in this view. To return to normal view, click Timeline again.

View Audit Activity at a Glance

Select the **Auditor for SQL Server** node to view SQL Server audit activity on the Activity dashboard.

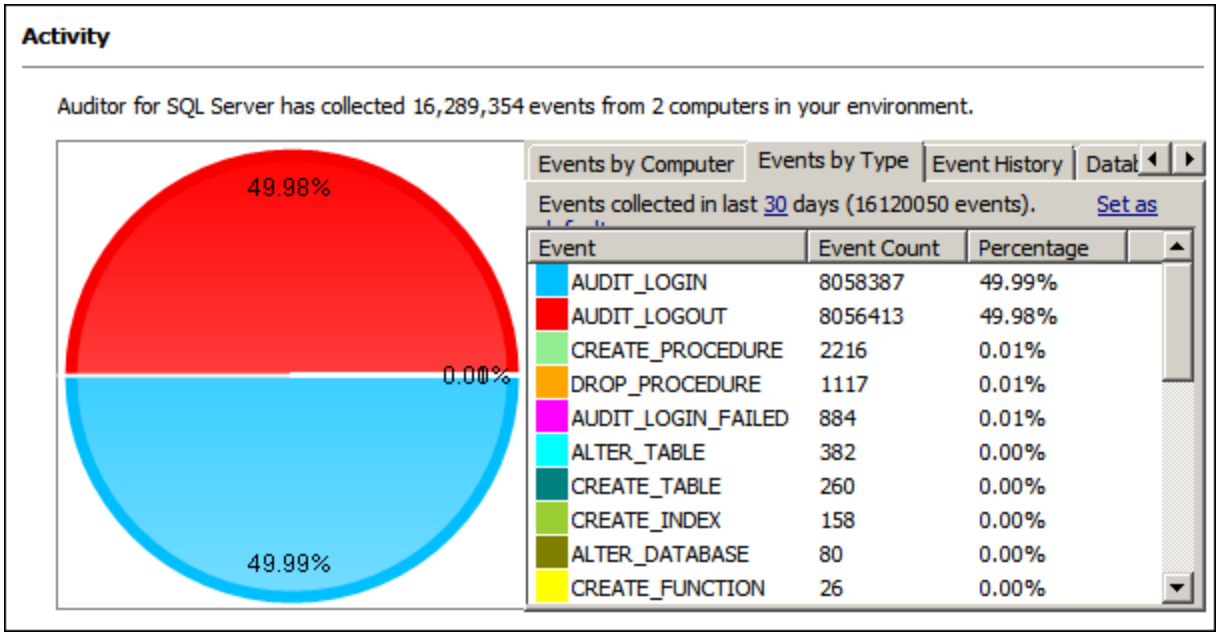
Events by Computer



The Events by Computer tab provides a high-level database overview with the number of monitored events per SQL server.

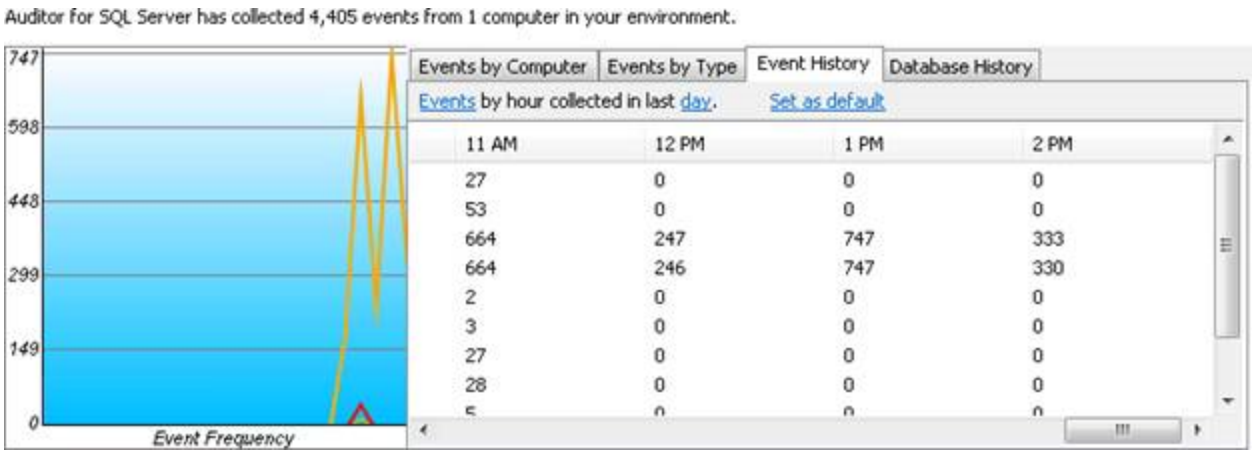
Click an underlined value to edit the value. For example, click the <*days*> value to choose a different time range.

Events by Type



The Events by Type tab breaks down the type of event for all servers monitored. Click the underlined value to set a different time range.

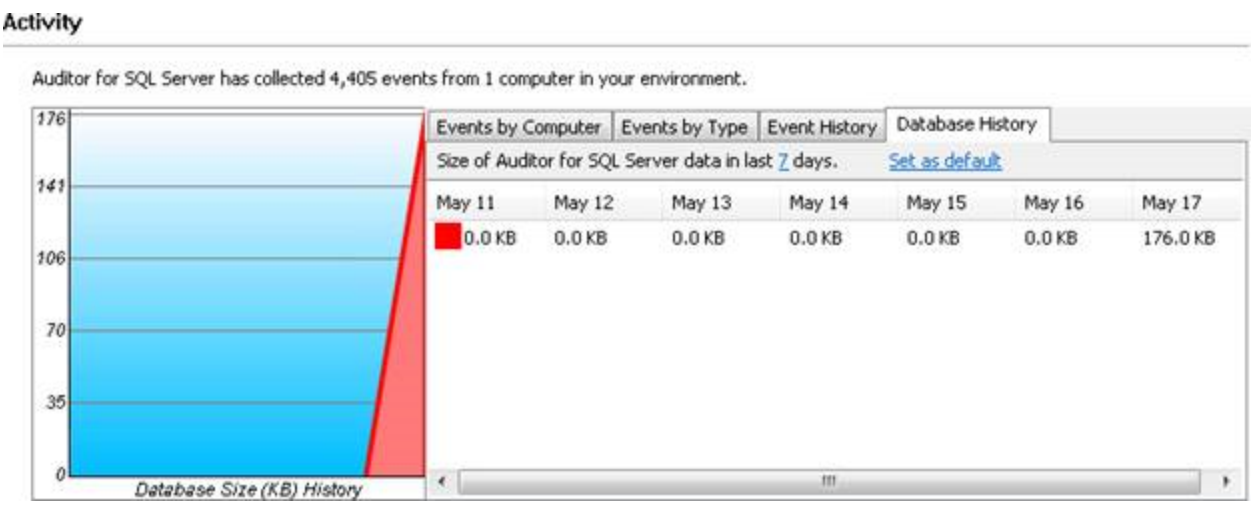
Event History



The Event History tab shows the frequency of different events for a particular time range. Click the underlined value to set a different time range or event.

Note: If you are monitoring login and logout events, you may want to exclude these events from the graph to ensure data is displayed as expected.

Database History



The Database History tab shows the growth of the database for a particular time range. Click the underlined value to set a different time range.

Work with Reports

Reporting is provided through Microsoft SQL Server Reporting Services (SSRS). SSRS needs to be implemented and configured before you can deploy reports.

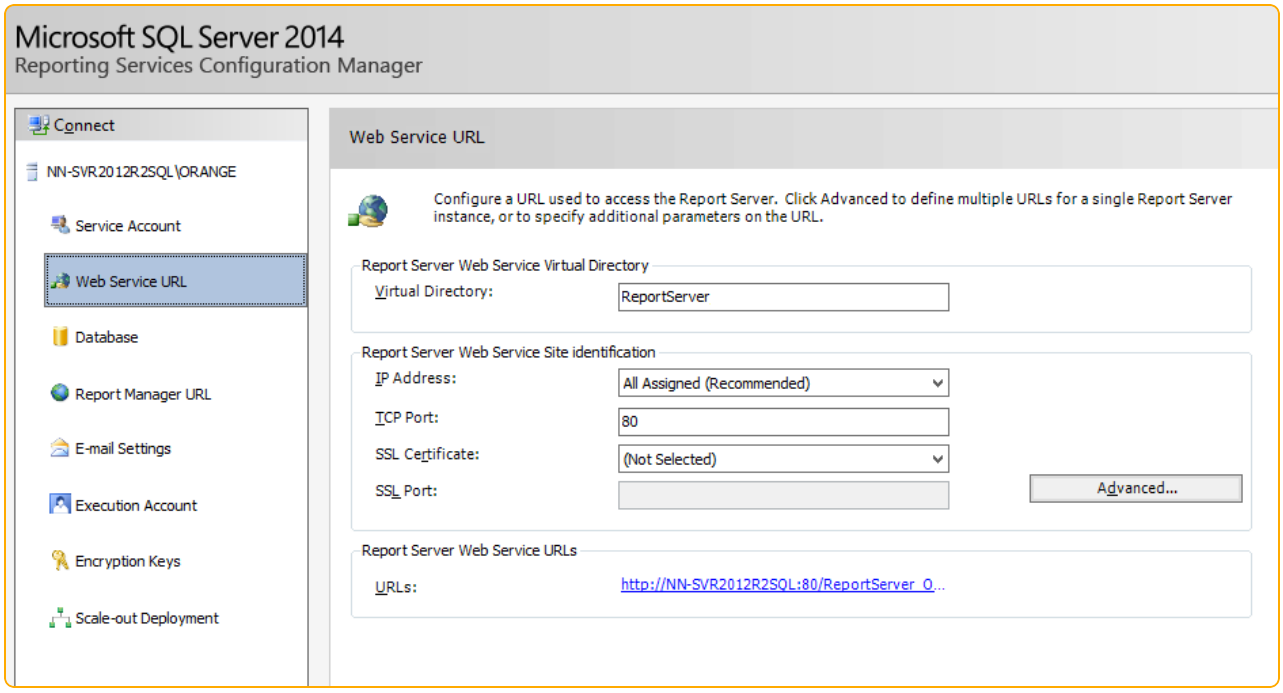
For more information, please see Microsoft's SSRS documentation for installation and configuration procedures.

Before Deploying Reports

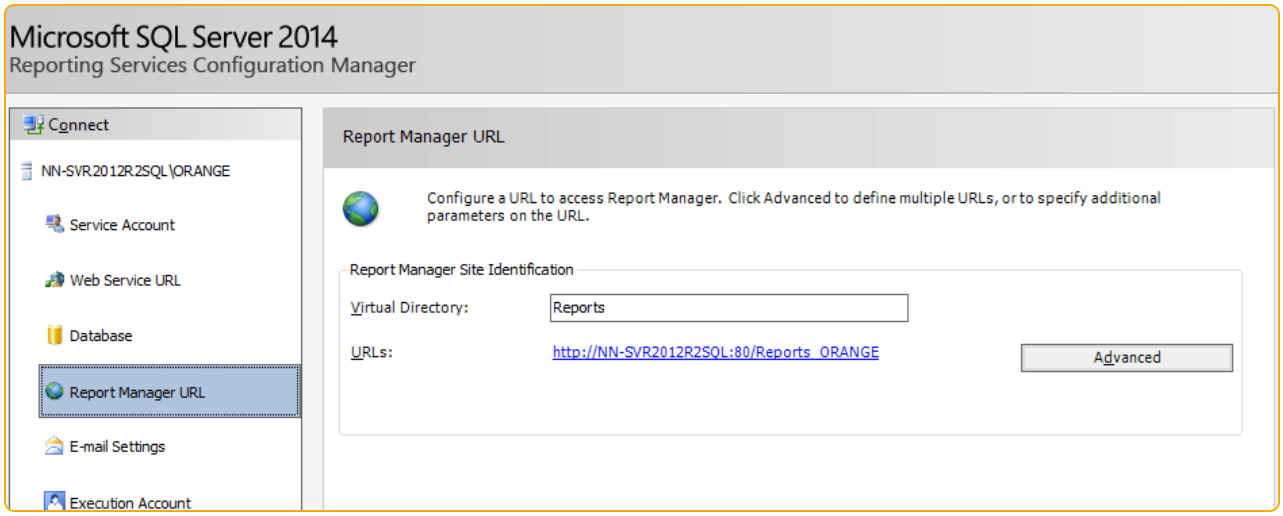
Before you deploy reports to SSRS, you need to know the Web Service URL and the Report Manager URL. You configure the settings when you initially set up SSRS.

Open the SQL Server Reporting Services Configuration Manager, and make note of the URLs.

Web Service URL



Report Manager URL



Deploy Reports

1. Select the **Cygna Auditor for SQL Server** node.
2. Click the Click here to configure reports link in the right pane.
3. The Reporting Services Configuration dialog box opens.
   - If reports are deployed, the fields will be completed.
   - If reports are not deployed, the fields will be empty.
4. Enter the Web Service and Report Manager URLs, and then click Connect.
5. Click OK when a successful connection is made. Now the version string is displayed.
6. The Folder box displays the default path for the reports on the server. Click Browse to change the path, if necessary.
7. Click Deploy to upload the reports.
8. Click OK in the Success dialog box.

Note: You can change the reporting configuration after the reports are deployed by clicking Click here to configure reports in the Auditor for SQL Server dashboard.

View Reports

1. Double-click an audit view to open the SQL Server Viewer.
2. Click Open Reports on the Home tab.
3. The default browser opens and shows the Report Manager URL. Click a report.

Note: This is a static URL for all Auditor for SQL reports. Bookmark it for quick reference in the future.

4. If prompted, set the report parameters and click View Report.
5. The report loads.

Built-In Reports

The following Auditor for SQL reports are available.

Report Name	Report Description
All Audit Events Summary	View a summary report of all audit events.
All SQL Server Changes	View all SQL server audit activity.
Deleted SQL Server Objects	View deleted objects, such as tables, indexes, and procedures.
Events by Database	View a summary report of events by SQL server and database.
Events by Database and Type	View a summary report of events by SQL server, database, and event type.
Events by Type	View a summary report of events by event type.
Failed Login Attempts	View failed login attempts.
Function Changes	View all creations, deletions, and modifications performed on functions.
Index Changes	View all creations, deletions, and modifications performed on indexes.
Login Changes	View all creations, deletions, and modifications performed on SQL server logins.
Modified SQL Server Objects	View modified objects, such as tables, indexes, and procedures.
Newly Created SQL Server Objects	View objects (such as tables, indexes, and procedures) that have been created in the past seven days.
Procedure Changes	View all creations, deletions, and modifications performed on

Report Name	Report Description
	functions.
Server Instance Changes	View changes to the SQL server global configuration settings. Not available for SQL Server 2005.
Server Role Changes	View when members have been added to or removed from a SQL server role.
Server Summary	View a summary report of event count by database and by type.
Table Changes	View all creations, deletions, and modifications performed on tables.
User Changes	View all creations, deletions, and modifications performed on users.
View Changes	View all creations, deletions, and modifications performed on views.

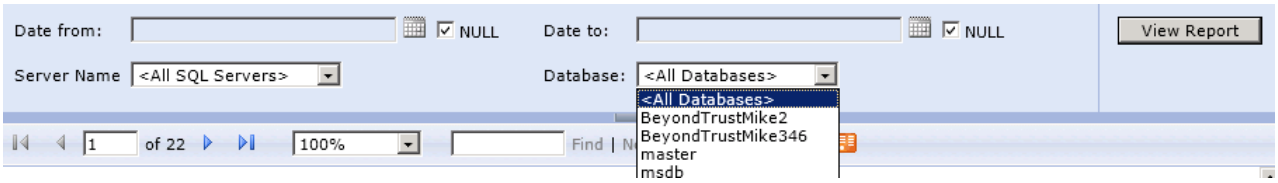
Manage Reports

SQL Server Reporting Services features are available for Auditor for SQL reports.

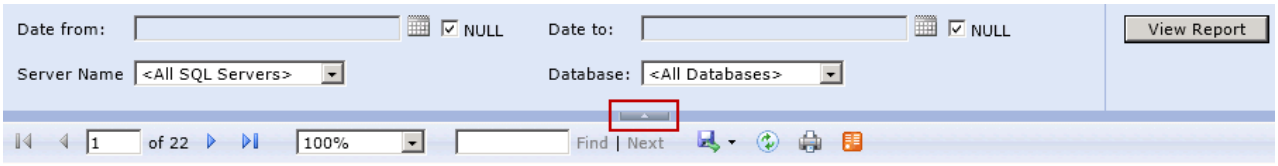
1. To manage reports, move your mouse over the title of the report and click the arrow.
2. Choose an option from the menu.

Use Report Features

Run a Report Immediately



In any report, you can change the parameters at the top to filter your view. Click View Report after changing parameters to refresh the data.



To hide the parameters area, click the small gray arrow below the pane.

Reporting Toolbar

Between the parameter area and the report data, you will see a toolbar.

Toolbar commands

COMMAND	DESCRIPTION
	Move to the first page or the last page (outer arrows) or ahead or back one page (inner arrows). You can also type a page number in the text box to view.
	Change the zoom level of the report.
	Type a search term (here we have used ALTER) and click Find to view the first instance. Click Next to view the next instance.
	Export report data into a variety of formats, including PDF, Excel, and Word.

COMMAND	DESCRIPTION
	Refresh the report.
	Print the report.
	Export this report to a data feed.

Sort Table Data

To sort table data, click the arrows in the appropriate column header.

Drill Into Reports

If data in a cell is underlined, click it to view more information on that specific item.

Note: Some reports not accessible from the main Reporting Services page are available in this way.

If you see the  icon at the beginning of a row, click it to view details for that event.

Here are the details for the event shown on the previous page.

Note the + and – signs in the report section headers (Standard Properties, SQL Text, and Additional Properties). These icons allow you to collapse or expand the respective section.

Set Report Parameters

A best practice approach is to narrowly scope the report. Otherwise, a significant amount of data can be generated. This may exceed the timeout configuration for SSRS.

1. Open the Auditor for SQL reports URL. For more information, please see View Reports.
2. Click the options arrow for any report and click Manage.
3. Click the Processing Options category. Modify the options in the Report Timeout section, as needed.
4. Click Apply to commit your changes.

Create Custom Reports

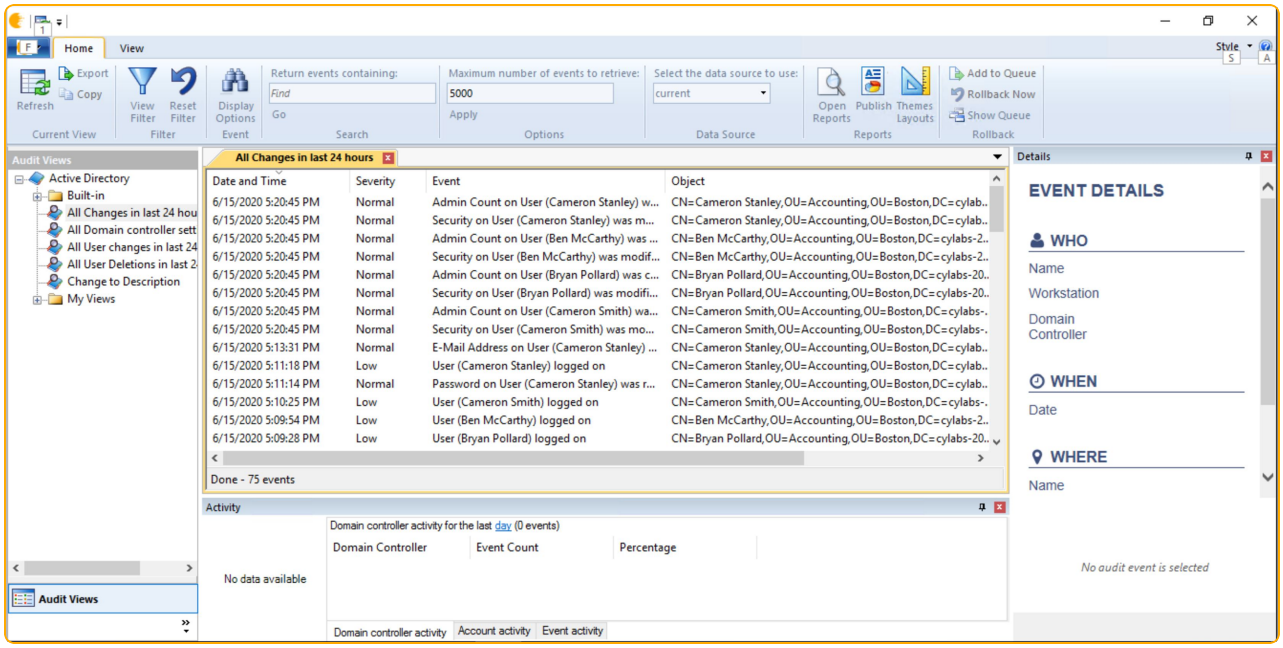
The custom report is based on the settings from the audit view you created. Be sure your report server is already configured to be used with Auditor. For more information, please see Deploy Reports.

Set the Layout

You can customize the look of your reports, choosing color palettes, report logo, and report output sizes.

To set up the layout for a report:

1. Open the Audit Viewer.



2. Select an Audit View and click Layout Themes.
3. Click the Themes tab.
4. Click Create Theme link.
5. On the Images page, click Add Custom Image to add your report logo. The maximum image size is 255x65 pixels.
6. On the Colors page, select the color palette for your report display.
7. Click Show Preview to see the changes in a demo report. You can have the Preview page open at the same time as you select colors from the palette to see the changes dynamically.
8. Click the Layouts tab.

9. Click the Create Layout link.
10. On the General page, enter a name and description.
11. On the Report Size page, click the Web Display tab to set online viewing properties.
12. Select a screen size from the list.
13. Alternatively, click the Show Advanced Options to set a custom size width and height for your display.
14. Select the Print Display tab to set print viewing properties.
15. On the Columns page, select the columns that you want to display in the report.

Publish the Report

1. Select the Audit View and click Publish.
2. The Custom SSRS Report Publisher dialog box opens.
3. On the General page, enter a report name and description.
4. Select the Sync with Audit View check box. Synchronize the audit view and the custom report to republish the report when the audit view data changes.
5. Select a layout and theme if you created custom settings for the report properties. For more information, please see Set the Layout.
6. On the Analytics page, select the graph data you want to see in the report.
7. On the Overview page, select the report server.
8. Click the Change Folder link to save the report to an alternate location.
9. Select the Publish print report check box to publish the report to SSRS using the print sizes selected on the Layout page. Click the Change Folder link to set another location in SSRS (if needed).
10. Click Publish.
11. A message is displayed indicating the report is generated and available in SSRS.
12. After the report is generated, click Open to view the report results in SSRS.